PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Michael WRAY**	Examiner:	Andrew L. NALVEN
Serial No.:	**09/732,954**	Art Unit:	2134
Filed:	December 7, 2000	Our Ref:	B-4053 618409-8
For:	"METHOD AND APPARATUS FOR DISCOVERING A TRUST CHAIN IMPARTING A REQUIRED ATTRIBUTE TO A SUBJECT"	Date:	April 28, 2005
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated January 28, 2005, for the above identified patent application. The Notice of Appeal is filed concurrently, together with an authorization to charge the requisite fee, and a courtesy copy is attached hereto. Please charge the amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief to deposit account no. 08-2025. An Amendment After Final Rejection pursuant to 37 C.F.R. 1.116 is also submitted concurrently, and a courtesy copy is attached herewith. Entry of this Amendment prior to consideration of the present Brief is respectfully requested, because the Amendment solely corrects multiple dependency errors in the pending claims, thereby presenting the claims in better form for consideration on appeal.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA.

STATUS OF CLAIMS

Claims 1 - 36 are the subject of this Appeal and are reproduced in the accompanying appendix as currently pending, prior to entry of the Amendment After Final Rejection filed concurrently herewith.

STATUS OF AMENDMENTS

An Amendment After Final Rejection has been submitted concurrently herewith, entry of which is respectfully requested.

SUMMARY OF THE CLAIMED INVENTION

The present application discloses methods and systems for discovering a trust chain that imparts a required attribute to a subject and that is grounded in a known trusted issuer (p. 1, ll. 6-7). The attributes are imparted or delegated through certificates (p. 1, ll.21-29). This can be a complicated task when many certificates are available but only some of which are relevant to the goal (the trust chain) that is desired to be discovered. The claimed invention does so by taking the goal to be proved, which is the delegation of an attribute (which may be any capability, characteristic or authorization – p. 1, ll. 9-12) from the known trusted issuer to the subject (who can thus be seen as the beneficiary of that delegation as the issuer has now bestowed a certain capability or authorization onto the subject), and decomposing this primary goal into subgoals. One of these subgoals corresponds to the delegation of an attribute by a certificate that is available and also has the same subject (p. 6, ll. 9-14). This is a recursive process that backtracks to a previous subgoal whenever a subgoal that has not been proved (by an axiom, or trusted assumption, corresponding to delegations from the trusted issuer to trusted principals – p. 6, ll. 19-21) cannot be further decomposed. Subgoals not justified by an available certificate are further decomposed, and one of the resulting further subgoals must correspond to the delegation of an attribute by a certificate that is available and that has the same subject as the subgoal from which it was decomposed (p. 6, ll. 10-14). The process is complete when the only subgoal

remaining is justified by a justified attribute delegation from the known trusted issuer (p. 6, ll. 15-18). Thus, it is important to appreciate that the process of the invention seeks a backward proof, in that it does not start with the first link in the trust chain (which is an axiom, or trusted delegation) but rather with the desired conclusion (the delegation to the subject) which it then tries to justify by the above-described backwards proof process (p. 8, ll. 23-26). In other words, the trust chain is built up, one subgoal at a time, **from** the subject **to** the known trusted issuer.

ISSUES

Issue 1: Whether Claims 1-36 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 6,134,550 to Van Oorschot (hereinafter "Van Oorschot") in view of The Book of Applied Cryptography by Menezes et al. (hereinafter "Menezes").

THE ARGUMENT

Issue 1: Whether Claims 1-36 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 6,134,550 to Van Oorschot (hereinafter "Van Oorschot") in view of The Book of Applied Cryptography by Menezes et al. (hereinafter "Menezes").

In section 6 of the final Office Action of February 23, 2005, the Examiner asserts that Van Oorschot discloses all claimed limitations of claims 1, 13 and 25, with the exception of the seeking of a backwards proof, and that Menezes teaches the seeking of a backwards proof of a primary goal precisely as set out in Appellant's claim 1. The Examiner thus opines that it would have been obvious to one of ordinary skill in the art to utilize Menezes' method of using backtracking proofs because doing so offers the advantage of removing the need for a central trusted authority.

Appellant has reviewed the two references with care, paying particular attention to the passages cited to by the Examiner, and is compelled to disagree with the Examiner's

understanding of these references. Claim 1 includes the limitation of "seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter." Contrary to the Examiner's assertion, there is absolutely no disclosure in Menezes of the concept of seeking a backwards proof of a trust chain, that is, seeking a proof by starting with the subject and proving the chain backwards to the issuer.

It is likely that the Examiner is misled by Menezes' use of "reverse certificates," which are created by a non-root node in a hierarchy of Certificate Authorities (CAs) by signing the public key of its immediate parent CA in the hierarchy. Figure 13.9(d) illustrates such a hierarchy with reverse certificates being depicted by the upward pointing arrows, and the typical "forward certificates" where a parent CA signs the public key of a child CA depicted by the downward pointing arrows. As explained on page 572, section (i), a verifier wishing to obtain trust in a public key can do so if "*a chain of certificates* can be constructed which corresponds to an unbroken chain of trust from the CA public key which the verifier does trust to the public key it wishes to obtain trust in." (emphasis in the original)

Menezes does not actually teach how the reverse certificates are used to construct this "chain of certificates" needed to establish a desired trust chain. However, the first sentence below the definition of "reverse certificate" on page 575 clearly states that "[i]n this model, each entity starts not with the public key of the root, but rather with the public key of the CA which created its own certificate, i.e. its local CA (parent). All trust chains now begin at an entity's local CA." The "entity" is a user entity (see Figure 13.9) and thus according to Menezes, the user entity is provided with the public key of its local CA - and will therefore trust any certificate it can verify as being signed by this CA. Thus, if a user entity A (which, in this context, corresponds to Appellant's "known trusted issuer") wants to know if it can trust the public key of another user entity B (that key being one certified by another CA in the hierarchy), the entity A must establish a trust chain from itself to the entity B by constructing a chain of certificates via its local CA and other CAs in the hierarchy. To construct this chain of certificates, entity A will

need to use "reverse certificates" as well as "forward certificates" to move up and down the CA hierarchy, as set forth by Menezes in the second sentence below the definition of "reverse certificate" on page 575: "[t]he shortest trust chain from any entity A to another entity B is now the path in the tree which travels upwards from A to the least-common-ancestor of A and B, and downwards from that node on to B." Thus, Menezes makes quite clear that the trust chain is established from the entity A to the entity B, not starting with entity B and working backwards to entity A as per Appellant's claim 1.

This aspect of Menezes' method is reinforced throughout the document: "[t]he goal is to find a sequence of certificates corresponding to a directed path... starting at the node corresponding to the CA whose public key the verifier trusts a priori and ending at the CA which has signed the certificate of the public key to be verified." (page 572, last full paragraph); "[i]n the absence of more advanced techniques or routing tables, any existent certification path could be found by depth-first or breadth-first search of the reverse certificates in cross-certificate pairs starting at the CA whose public key the verifier possesses initially" (page 573, second full paragraph) (emphasis added).

Appellant is mindful of the requirements posited by MPEP 2143.03 that "[t]o establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). All words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)." (emphasis added) Thus, Appellant respectfully contends that the Examiner has not made, and indeed cannot make, a *prima facie* showing that combining Van Oorschot with Menezes would yield the claimed method, because neither of these references discloses or alludes to the backwards proving of an attribute delegation as recited in claim 1. Appellant therefore respectfully requests that the rejection of claim 1 be overturned on appeal.

Claims 2-12 depend from claim 1. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 1, Appellant submits that claims 2-12 are also allowable, and respectfully requests that the rejection of these claims be overturned.

Claim 13 is a system claim and claim 25 is a computer program product claim corresponding to method claim 1, and the above discussion of Van Oorschot and Menezes with respect to claim 1 is therefore equally relevant to the patentability of claims 13 and 25. Appellant therefore submits that claims 13 and 25, and claims 14-24 and 26-36 dependent therefrom respectively, are therefore also allowable, and respectfully requests that the rejection of these claims be overturned.

CONCLUSION

For the extensive reasons advanced above, Appellant respectfully contends that each pending claim is patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

April 28, 2005
(Date of Transmission)

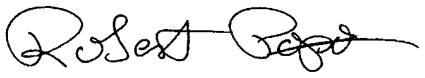
Mia Kim
(Name of Person Transmitting)

(Signature)

4/28/05
(Date)

Attachments

Respectfully submitted,



Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com

Claims

1. (previously presented) A method for discovering a trust chain, wherein the trust chain comprises at least attribute delegations each with an issuer and a subject, overall imparts a required attribute to a subject, and is grounded in a known trusted issuer, and wherein certificates are used as justification of associated attribute delegations, the method comprising:

a) setting as a primary goal to be proved an attribute delegation from a known trusted issuer to said subject;

b) seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter; and

c) determining that a trust chain has been found upon the process of (b) producing a chain of subgoals that is proved by corresponding certificates and that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal.

2. (previously presented) A method according to claim 1, wherein the known trusted issuer included in said primary goal

is a specifically identified entity that is inherently trusted by the discovery method at least in relation to said required attribute, said justified attribute delegation being an attribute delegation that is justified by a corresponding certificate.

3. (previously presented) A method according to claim 1, wherein the known trusted issuer included in said primary goal is the discovery method itself; said justified attribute delegation being an attribute delegation that is justified either by an axiom inherently trusted by the discovery method, or by a corresponding certificate.

4. (original) A method according to claim 3, wherein the discovery method, as said known trusted issuer, is represented in said primary goal and said axiom as a null issuer.

5. (previously presented) A method according to claim 1, wherein name mappings justified by corresponding certificates are permitted in a said trust chain in addition to attribute delegations, and wherein the process of (b) further comprises:

decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

6. (previously presented) A method according to any one of the preceding claims, wherein seeking a backwards proof further comprises:

maintaining a list of subgoals already generated and pursued, checking each new subgoal against said list, and terminating the process of seeking of a backwards proof in failure in the event of a new subgoal being found to already exist in the list.

7. (previously presented) A method according to any one of the preceding claims, wherein at least some of said certificates used in proving a determined trust chain as found have associated validity data, the method comprising the further step of traversing the trust chain in a forwards direction from the trusted attribute delegation that grounds it and combining the validity data of all certificates involved to determine the validity of the overall attribute delegation represented by the chain.

8. (previously presented) A method according to claim 7, wherein determining that a trust chain has been found comprises storing the state of the seeking of a backwards proof prior to checking the validity of the trust chain found, this state being used to continue the process should the check of the validity of the initially found chain show that the chain is not valid.

9. (previously presented) A method according to any one of the preceding claims, wherein an attribute-delegation certificate used to prove a said subgoal has a subject-directed condition associated with it requiring that a specified subject must have a particular attribute in order for the delegation to be valid, and wherein the process of (b) further comprises:

making said subject-directed condition a further subgoal to be proved for the current chain being followed.

10. A method according to claim 1, wherein the process of step (b) is run to completion to find all trust chains, if any, proving the primary goal.

11. (previously presented) A method of selecting certificates to be sent to a resource which requires proof that a subject has a particular attribute before allowing use of the resource, comprising:

finding a trust chain by the method of any one of claims 1 to 7 in respect of said subject and an issuer known, or likely, to be trusted by said resource; and

selecting for sending to said resource certificates associated with a trust chain, if any, thereby found.

12. (previously presented) A method of determining whether a resource requiring a user to have at least one predetermined

attribute, is usable by a subject presenting certificates to the resource, comprising:

finding a trust chain by the method of any one of claims 1 to 7 in respect of said subject and an issuer known and trusted by said resource; and

determining that use of the resource by the subject is permitted if a trust chain can be found.

13. (previously presented) A system for discovering a trust chain, wherein the trust chain comprises at least attribute delegations each with an issuer and a subject, overall imparts a required attribute to a subject, and is grounded in a known trusted issuer, and wherein certificates are used as justification of associated attribute delegations, the system comprising a processor for:

setting as a primary goal to be proved an attribute delegation from a known trusted issuer to said subject;

seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter; and

determining that a trust chain has been found upon

producing a chain of subgoals that is proved by corresponding certificates and that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal.

14. (previously presented) A system according to claim 13, wherein the known trusted issuer included in said primary goal is a specifically identified entity that is inherently trusted at least in relation to said required attribute, said justified attribute delegation being an attribute delegation that is justified by a corresponding certificate.

15. (previously presented) A system according to claim 13, wherein the known trusted issuer included in said primary goal is a discovery method of the system itself; said justified attribute delegation being an attribute delegation that is justified either by an axiom inherently trusted by the discovery method, or by a corresponding certificate.

16. (previously presented) A system according to claim 15, wherein the discovery method, as said known trusted issuer, is represented in said primary goal and said axiom as a null issuer.

17. (previously presented) A system according to claim 13, wherein name mappings justified by corresponding certificates

are permitted in a said trust chain in addition to attribute delegations, and wherein seeking a backwards proof further comprises:

decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

18. (previously presented) A system according to any one of claims 13-17, wherein seeking a backwards proof further comprises:

maintaining a list of subgoals already generated and pursued, checking each new subgoal against said list, and terminating the process of seeking a backwards proof in failure in the event of a new subgoal being found to already exist in the list.

19. (previously presented) A system according to any one of claims 13-18, wherein at least some of said certificates used in proving a determined trust chain as found have associated validity data, the processor further for traversing the trust chain in a forwards direction from the trusted attribute delegation that grounds it and combining the validity data of all certificates involved to determine the validity of the overall attribute delegation represented by the chain.

20. (previously presented) A system according to claim 19, wherein determining that a trust chain has been found comprises storing the state of the seeking of a backwards proof prior to checking the validity of the trust chain found, this state being used to continue the process should the check of the validity of the initially found chain show that the chain is not valid.

21. (previously presented) A system according to any one of claims 13-20, wherein an attribute-delegation certificate used to prove a said subgoal has a subject-directed condition associated with it requiring that a specified subject must have a particular attribute in order for the delegation to be valid, and wherein seeking a backwards proof further comprises:

making said subject-directed condition a further subgoal to be proved for the current chain being followed.

22. (previously presented) A system according to claim 13, wherein the seeking of a backwards proof is run to completion to find all trust chains, if any, proving the primary goal.

23. (previously presented) A system according to any one of claims 13-18, wherein said processor is further for selecting certificates to be sent to a resource which requires proof that a subject has a particular attribute before allowing use of the resource by:

finding a trust chain in respect of said subject and an

issuer known, or likely, to be trusted by said resource; and

selecting for sending to said resource certificates associated with a trust chain, if any, thereby found.

24. (previously presented) A system according to any one of claims 13-18, wherein said processor is further for determining whether a resource requiring a user to have at least one predetermined attribute is usable by a subject presenting certificates to the resource, by:

finding a trust chain in respect of said subject and an issuer known and trusted by said resource; and

determining that use of the resource by the subject is permitted if a trust chain can be found.

25. (previously presented) A computer program product for use in connection with a computer for discovering a trust chain, wherein the trust chain comprises at least attribute delegations each with an issuer and a subject, overall imparts a required attribute to a subject, and is grounded in a known trusted issuer, and wherein certificates are used as justification of associated attribute delegations, said computer program product comprising a computer-readable medium having encoded thereon instructions for:

setting as a primary goal to be proved an attribute delegation from a known trusted issuer to said subject;

seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter; and

determining that a trust chain has been found upon producing a chain of subgoals that is proved by corresponding certificates and that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal.

26. (previously presented) A computer program product according to claim 25, wherein the known trusted issuer included in said primary goal is a specifically identified entity that is inherently trusted at least in relation to said required attribute, said justified attribute delegation being an attribute delegation that is justified by a corresponding certificate.

27. (previously presented) A computer program product according to claim 25, wherein the known trusted issuer included in said primary goal is a discovery method itself; said justified attribute delegation being an attribute delegation that is justified either by an axiom inherently trusted by the discovery method, or by a corresponding certificate.

28. (previously presented) A computer program product according to claim 27, wherein the discovery method, as said known trusted issuer, is represented in said primary goal and said axiom as a null issuer.

29. (previously presented) A computer program product according to claim 25, wherein name mappings justified by corresponding certificates are permitted in a said trust chain in addition to attribute delegations, and wherein seeking a backwards proof further comprises:

decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

30. (previously presented) A computer program product according to any one of claims 25-29, wherein seeking a backwards proof further comprises:

maintaining a list of subgoals already generated and pursued, checking each new subgoal against said list, and terminating the process of seeking a backwards proof in failure in the event of a new subgoal being found to already exist in the list.

31. (previously presented) A computer program product according to any one of claims 25-30, wherein at least some of said certificates used in proving a determined trust chain as found have associated validity data, the method further comprising traversing the trust chain in a forwards direction from the trusted attribute delegation that grounds it and combining the validity data of all certificates involved to determine the validity of the overall attribute delegation represented by the chain.

32. (previously presented) A computer program product according to claim 19, wherein determining that a trust chain has been found comprises storing the state of the seeking of a backwards proof prior to checking the validity of the trust chain found, this state being used to continue the process should the check of the validity of the initially found chain show that the chain is not valid.

33. (previously presented) A computer program product according to any one of claims 25-32, wherein an attribute-delegation certificate used to prove a said subgoal has a subject-directed condition associated with it requiring that a specified subject must have a particular attribute in order for the delegation to be valid, and wherein seeking a backwards proof further comprises:

making said subject-directed condition a further subgoal to be proved for the current chain being followed.

34. (previously presented) A computer program product according to claim 25, wherein the seeking of a backwards proof is run to completion to find all trust chains, if any, proving the primary goal.

35. (previously presented) A computer program product according to any one of claims 25-30 and further for selecting certificates to be sent to a resource which requires proof that a subject has a particular attribute before allowing use of the resource, by:

finding a trust chain in respect of said subject and an issuer known, or likely, to be trusted by said resource; and

selecting for sending to said resource certificates associated with a trust chain, if any, thereby found.

36. (previously presented) A computer program product according to any one of claims 25-30 and further for determining whether a resource requiring a user to have at least one predetermined attribute is usable by a subject presenting certificates to the resource, by:

finding a trust chain in respect of said subject and an issuer known and trusted by said resource; and

determining that use of the resource by the subject is permitted if a trust chain can be found.